Hogan Lovells

FiDA Impact Report

October 2025

1. Introduction

1.1 The Second Payments Services Directive ((EU) 2015/2366) ("**PSD2**") provided payment service users with access to their payment data by mandating that payment service providers grant "read" and (limited) "write" access over payment accounts to "third party providers" ("**TPPs**") acting at the data owner's request.

1.2 The draft text for the EU Financial Data Access Regulation ("**FiDA**") extends the scope of such read access, beyond payment account data, to include a broader range of financial services—such as credit agreements, savings, investments, pensions, insurance (excluding health/life), and crypto-assets.

1.3 Similar to the data sharing aspects of PSD2, FiDA's overarching aim is to:

(a) enable customers to benefit from their financial data and help them to make informed financial decisions;

(b) mandate data sharing between financial institutions and third-party providers to drive innovation and produce more "customer-centric" products; and

(c) increase competition between financial service providers, to increase consumer choice and lower pricing.

1.4 Some of the proposed framework borrows directly from the world of payments regulation (current and future), incorporating:

(a) a statutory right of access for customers ("**data owners**") to access data held by financial institutions ("**data holders**") via other service provider parties ("**data user**s");

(b) data user access being dependent on explicit, informed, purpose-specific, revocable customer consent;

(c) the concept of an information sharing service as a regulated activity that can be provided by authorised TPPs; and

(d) dashboards provided by data holders to enable customers to review and update their TPP access consents.

1.5 However, despite certain similarities, FiDA is more than a simple expansion of the PSD2 model for data sharing. Rather, it marks an evolution in terms of how consumers may benefit from access to their financial data, partly derived from lessons learnt during the implementation of PSD2 and the emergence and continued disruption of "big tech" in financial services.

1.6 Once the European Commission published its original draft (the "**Commission Text**") on 28 June 2023, the European Parliament and Council published their respective versions (the "**Parliament Text**" on 30 April 2024 and the "**Council Text**" on 2 December 2024).

1.7 Following the first trilogue session, the Commission subsequently produced a "Simplification Non-Paper" (17 May 2025) to facilitate discussions in the subsequent trilogue sessions.

1.8 It is anticipated that the trilogue process will result in a finalised text by the end of this year under the Danish presidency.

1.9 This impact report highlights some of the key changes FiDA will introduce, as wells as some of the critical issues raised by the regulation.

2. Scope – Who (Article 2)

2.1 Whereas PSD2 applied only to payment service providers in respect of payment account data, FiDA applies to almost all other financial services firms in respect of the customer data they hold.

2.2 Such firms are both "data holders" required to provide access to customer data and "data users", entitled to access such data at the express request of the customer.

2.3 FiDA also introduces a new type of financial services provider in the form of a **"Financial Information Service Provider"** or **"FISP"** – a TPP whose service is to collate/aggregate/access non-payment account customer data at the request of the data owning customer.

Data holders and users (as proposed by the Commission Text)

Data Holders	Data Users
Banks	All data Holders
Insurers and Insurance intermediaries	FISPs
Investment Firms and Brokers	
Payment Institutions/ Electronic money institutions	
Loan companies (mortgages, loans, etc.)	
Pension Funds	
Cryptoasset service providers (CASPs) and Asset Referenced Token issuers	
Credit reference agencies	
Crowdfunding service providers	

2.4 Unlike PSD2, which sought to bring an activity that was already occurring in the payment's ecosystem within the scope of regulation, interestingly, FiDA is using regulation to drive new services and innovation in respect of customer financial data.

2.5 Only FISPs are required to apply for authorisation to operate as data service users, with already-regulated financial institution data holders being able to take advantage of their existing status as regulated entities (albeit with a light-touch notification process suggested in the Council Text).

2.6 Given the plurality of institutions to which the regulation applies, FiDA drastically expands the scope of data aggregation and the possibilities that having access to such data offers. Whilst FiDA deliberately excludes highly sensitive categories such as health-related insurance, personal injury claims, consumer credit scoring outputs, and proprietary data derived by providers, it opens up a wealth of financial data for data users to mine through access via Financial Data Sharing Schemes (FDSS) and with customer consent.

2.7 FiDA exempts certain categories of financial institutions, typically on the basis of their size. Specifically, the following will not be within scope:

(a) alternative investment fund managers with assets under €100m euros, or €500m euros that are unleveraged with no redemption rights for the first 5 years;

(b) insurers excluded from Solvency II due to their size;

(c) pension schemes which do not have more than 15 members in total;

(d) natural or legal persons excluded from MIFID; and

(e) insurance intermediaries which are microenterprises or small or medium-sized enterprises.

2.8 The trilogue process has revealed other possible reductions in scope favoured by the Parliament and Council, specifically:

(a) occupational pension providers (who would remain in scope only insofar as they manage personal pension products per the Council Text);

(b) credit rating agencies (deleted in the Parliament Text); and

(c) reinsurance undertakings (deleted in both) (and possibly ancillary insurance intermediaries, as per the Parliament Text).

2.9 The Council is also interested in excluding other entities for which FiDA-eligible activities represent only a marginal part of their total business.

2.10 The Commission (having had the benefit of seeing the other bodies' proposals) is alive to the issue but would prefer to introduce proportionality for smaller-sized entities, rather than exempt whole sectors, particularly occupational pension providers. Given the increasing fluidity of job moves, there is clearly merit in including such providers within scope to facilitate a customer's understanding of their pension position overall.

2.11 Scope – What (Article 2)?

2.12 There is, however, agreement among the legislators that access should be limited to consumer and SME data. This was not the case with PSD2, which did not extend the "corporate opt" (under which larger corporate customers could agree that certain payment services requirements would not apply to them) to the obligation to provide access to payment accounts and payment account data of corporate payment service users.

Given the increasing fluidity of job moves, there is clearly merit in including such providers in scope to facilitate a customer's understanding of their pension position overall.

2.13 In keeping with the categories of data holders that FiDA seeks to regulate, the Commission Text proposes that the following types of data shall be accessible to data users:

Data on.....	Comments
Mortgage credit agreements, loans, and accounts	Includes data such as balances, conditions, and transactions on accounts — **excluding payment accounts defined under PSD2**
Savings, investments, and other financial assets	Includes data gathered to perform suitability assessments
Financial instruments	Includes insurance-based investment products, crypto-assets, real estate, and related economic benefits
Pension Rights	Covers data from occupational pension schemes and pan-European personal pension products
Non-life insurance products	Excludes sickness and health insurance categories (sensitive health data explicitly excluded).
Creditworthiness assessment	Includes data gathered during loan application or credit rating processes, but excludes consumer creditworthiness assessment, AnaCredit Data[1] and firm's credit assessment output (e.g. credit score).

[1] AnaCredit stands for Analytical Credit Datasets—a data collection initiative by the European Central Bank (ECB). It gathers granular (loan-level) credit data from euro area banks to support, monetary policy analysis, financial stability monitoring, and banking supervision Although AnaCredit contains valuable credit data, it is collected for regulatory/supervisory purposes, not for commercial use and is not intended for sharing with third-party data users (like FinTechs or financial information services).

2.14 In addition to debating the extent to which certain institutions should be excluded, the trilogue discussions have focussed on the type of data to which in-scope entities must provide access, specifically relating to the age of the data in question, and the extent to which it is "live".

2.15 Specifically, the Parliament is proposing to limit access to the last 3 years' worth of data and is seeking to distinguish between terminated (i.e. no longer active) and fulfilled contracts to determine what data can be requested.

2.16 The Council proposes a more data-friendly approach, suggesting a 10-year limit on the age of data where the customer data is not readily available in digital format, or is not part of the contractual conditions of the product/service, and believes that including terminated contracts could facilitate year-on-year comparison.

2.17 The Commission appears to have some sympathy with the Council's position, but would prefer to exclude terminated agreements.

2.18 Further, the Parliament (but not the Council) would seek to exclude data collected as part of a creditworthiness assessment of a firm.

2.19 Scope – When (Article 36)?

2.20 The three EU bodies are also debating the time frame for the implementation of FiDA.

(a) The Commission Text provides for a 2-year implementation period, with the regulation taking effect 24 months after publication and requirements relating to the means through which data must be shared ("**Financial Data Sharing Schemes**" of "**FDSS**") and the FISP authorisation process coming into effect 6 months earlier.

(b) The Parliament Text pushes back the application of the provisions on FDSS and authorisation to the entities acting as data holders/data users to 3 years, with the remainder of the regulation becoming effective 2 months thereafter.

(c) The Council Text suggests a gradual approach, with implementation targets of:

(i) 2 years for personal loans, savings and motor insurance data;

(ii) 3 years for cryptoassets, mortgage, most investment, and personal pension scheme data; and

(iii) 4 years for non-consumer loan and credit-worthiness assessment, other insurance, and insurance-based investment data.

In each case, the authorisation and provisions on FDSS, etc, would come into effect 6 months earlier.

2.21 Clearly, specific industry sectors may welcome the opportunity to delay implementing FiDA. However, there is a risk that, in doing so, the general norms of FDSS requirements and accepted practice for data sharing are set by others coming into scope of FiDA in the earlier tranches.

"The Commission appears to have some sympathy with the Council position, but would prefer to exclude terminated agreements.

3. Use case I: Insurance

3.1 The following use case illustrates how access to financial data could benefit an insurer.

3.2 Such an insurer would:

(a) need to notify its supervising authority that it intends to act as a data user;

(b) obtain explicit consent from the policyholder to access their financial data for a specific purpose; and

(c) comply with all conduct, data protection, security, and use limitations set out in FiDA and GDPR.

3.3 Once these steps are completed, the insurer would be able to mine client data at other institutions, which would enable it to:

(a) discern coverage patterns, savings behaviour, and financial goals, enabling more personalised, modular insurance offerings;

(b) assess income changes in real-time allowing adjustments to premium support or risk classification; and

(c) access continuous financial data to enable dynamic risk models rather than relying solely on static, historical data, meaning it could price credit insurance, income protection, and health coverage more accurately.

3.4 Such understanding could enable usage-based or pay-as-you-go insurance models (such as a travel insurance product that activates automatically based on booking or payment data).

3.5 The insurer could also use customer data to improve its user experience and operational efficiency. For example, more granular data could help:

(a) reduce the risk of fraud and adverse selection (potentially leading to fairer pricing);

(b) streamline onboarding and automation through pre-filled forms using verified financial data (making customer onboarding faster and reducing drop-offs); and

(c) automate claims processing through verified financial transactions and third-party data sources.

3.6 FiDA also raises the prospect of cross-sector opportunities promoting an ecosystem approach, allowing insurers to collaborate more easily with FinTechs, wealthtechs, and banks and, possibly, smoothing the way to embedded insurance in a more scalable way —e.g., insurance offers directly embedded in banking apps.

4. Use Case II: Pension

4.1 Similarly, access to customers' complete financial data could enable a pension provider to:

(a) better understand financial goals;

(b) recommend suitable pension products; and

(c) offer integrated retirement planning.

4.2 Such data could enable a pension provider to:

(a) advise a user to increase contributions based on real-time income and spending patterns;

(b) design dynamic contribution plans (e.g. auto-adjust based on income);

(c) offer more targeted investment strategies based on risk tolerance and financial behaviour;

(d) prompt saving through real-time alerts to respond to changes in financial circumstances, such as missed contributions or drops in income, enabling a change in saving; and

(e) provide live information on pension planning and extrapolating future scenarios, providing customers with a clearer idea of their pension planning at an earlier stage in their career and how to improve their planning.

4.3 Since FiDA enables easy data sharing between pension providers (with customer consent), switching or consolidating pensions should become simpler, encouraging competition, efficiency, and better outcomes for savers.

4.4 It may also enable pension providers to partner more easily with banks (to embed pension services into banking apps), financial advisors and FinTechs (to offer bundled solutions), facilitating embedded pension planning in everyday financial management.

4.5 However, there remain some key areas of uncertainty in FiDA which need addressing to help deliver such benefits.

5. Areas of uncertainty

5.1 Current Account data

5.2 The elephant in the room is currently the exclusion of payment account data, as defined in PSD2, which appears in all three texts in one form or another in Article 2(1).

5.3 Since access to this data category is covered by PSD2, the legislators presumably did not see the need to cover access to this category of data in FiDA, designing open finance to complement open banking. However, there is an open question of what this means for non-bank data users/FISPs seeking this category of data, which is arguably the richest of the data sets out there:

(a) Will they need to become authorised under PSD2 as account information service providers ("**AISP**")?

(b) Will access under FiDA be similar in terms of the process, mechanics, and requirements as that for PSD2 (which focuses on eIDAS certificates, strong customer authentication ("**SCA**"), the ability to rely on underlying bank SCA protocols and certain exemptions from SCA being required in an AISP relationship)?

5.4 Currently, there is no obvious way of aligning the two regimes – although the Third Payment Services Directive ("**PSD3**") / Payment Services Regulation ("**PSR**") (also in trilogue) presents an opportunity to do so.

5.5 Similarly, the Parliament and Council Texts appear to exclude AISPs from being able to rely on their existing permission as a payment services provider to be able to act as a data user:

(a) while Article 2(2)(b) of the Commission Text specifically provides that categories of data holder include *"payment institutions, including account information service providers and payment institutions exempted pursuant to Directive (EU) 2015/2366"*, the latter part of this provision is excluded in both EP and Council Texts;

(b) both Texts include a further provision that an AISP *"may only access data under [FiDA] if it has been authorised as a financial information service provider"* (Article 12(4A) of the Parliament and Council Texts).

5.6 The Commission has suggested a possible compromise whereby a simplified authorisation process may be available for AISPs as part of the FISP authorisation process. Under this approach, certain information held on an entity registered as an AISP would not need to be re-submitted, and other core requirements for authorisation, like professional indemnity insurance, could be reused. It seems somewhat contradictory for a regulation that aims to enable third-party access to customer financial data to restrict entities that have already obtained regulatory approval to access one category of this data. It may be that that this is simply a reflection of the Parliament and Council not wanting to give one sector a competitive advantage.

5.7 However, FISPs (and AISPS) seem to be the only entities required to apply for specific authorisation under FiDA (Article 6(1)):

(a) the Commission and Parliament Text provide that a data user may access financial information data by virtue of their existing authorisation as a financial institution (an "**FI**") or where they are authorised as a FISP;

(b) the Council Text specifically provides that FI entities that qualify as data holders can provide financial information services following a light-touch notification process.

5.8 All three versions reinforce the natural advantage that credit institutions and other PSPs may enjoy, having:

(a) already implemented and lived a data sharing requirement since PSD2;

(b) (in most cases) embraced a digitalised means of engaging day-to-day with customers that skews heavily towards mobile phone interaction via apps; and

(c) the right to access payment account data under PSD2.

5.9 As a result, PSPs (being holders of payment account data, banks and EMIs in particular) have an advantage over other financial institutions, which would presumably need to become licensed as AISPs under PSD2, and integrate with the (separate) PSD2 data sharing model, in addition to those that FiDA will usher in.

5.10 Banks and EMIs are now uniquely positioned to leverage their new access rights to other financial institutions' data and serve as a one-stop shop for all their customers' data needs.

5.11 Third-country FISPS (Article 13 – Commission Text)

5.12 The Commission's proposals around third country FISPs (namely allowing authorisation of non-EU firms as FISPs, provided they appoint a legal representative in a member state) have been deleted in the Council and Parliament Texts.

5.13 Whilst this indicates a sensible caution over protecting EU customer data, it may also be part of a somewhat protectionist policy seen in other EU directives (including CRD VI , which requires third-country banks to establish branches within the EU or operate within certain, limited exemptions).

5.14 "Big Tech" (Recital 10, Articles 6(4b) and 12(4b) Parliament Text; Article s6(4b), 12(4b) and 18a Council Text)

5.15 Both the Parliament and Council Texts introduce limitations on the extent to which "Gatekeeper" entities may act as FISPs.

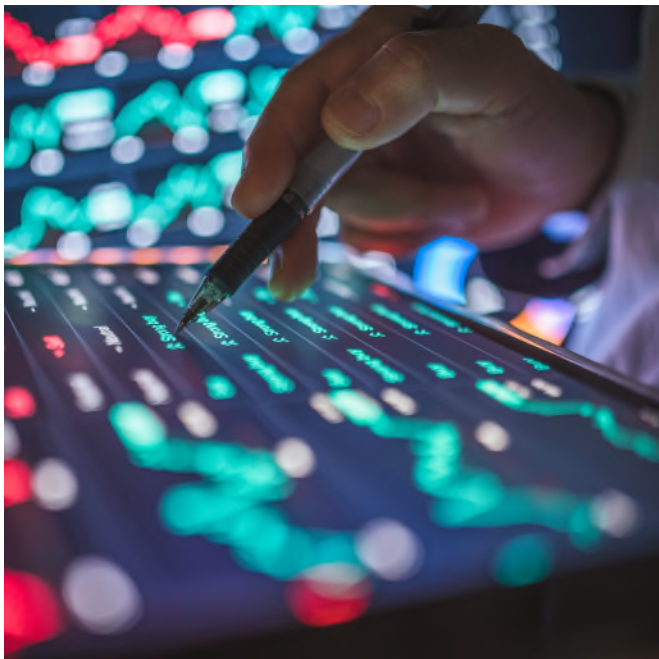
5.16 Entities classified as "gatekeepers" under the Digital Markets Act (primarily large tech firms) are:

(a) prohibited from becoming FISPs by the Parliament text (although a subsidiary may be established as a FISP); and

(b) subject to additional assessments to become authorised to engage in financial information services, and restrictions on combining financial information data with the wealth of data they may otherwise hold.

5.17 Both texts appear wary of tech giants wanting to access EU consumer data, whereas no such specific barrier/prohibition exists on tech companies becoming PISPs or AISPs.

5.18 Taken together with the removal of a third-country permission regime, the message appears to be that EU customer financial data should not be freely accessible to large overseas tech companies.



6. Financial data sharing schemes (Articles 9 – 11)

6.1 Whereas PSD2 looked to a regulator-driven governance model, FiDA looks to a market-driven solution to:

(a) define common technical standards and APIs;

(b) establish fair, transparent compensation models for data holders;

(c) define liability frameworks aligned with GDPR standards; and

(d) provide dispute-resolution mechanisms and governance rules.

6.2 Similarly, while standards were imposed as mandatory regulatory technical standards by regulators, FiDA looks to "optional", market-defined standards via FDSS.

6.3 In contrast, PSD2 did not create or recognise industry-consensus-based governance models. RTS defined the security, access, and communication protocols—such as the requirement to provide APIs or an equivalent interface (like a modified customer interface) and to comply with these standards by a fixed deadline. While some informal industry initiatives (e.g., Berlin Group, STET, and Open Banking in the UK) emerged to fill in technical details and API standards, these were not required or endorsed by PSD2 itself.

6.4 FiDA proposes a hybrid model that encourages market-led schemes with regulatory intervention only if the market cannot come up with one itself. Specifically, if no FDSS exist for specific data categories, the European Commission can step in via a delegated act to set standards, compensation models, and liability rules.

Given the treasure trove of financial data that data users will have access to, data security, the risk of unauthorised access and fraud, and liability for such access, are key concerns for FiDA's implementation

6.5 To a certain degree, FiDA tries to formalise what PSD2 left informal by:

(a) creating official channels (FDSS) for industry-led standard-setting;

(b) allowing regulatory intervention where markets do not cooperate; and

(c) aiming to prevent the fragmentation that TPPs faced under PSD2.

6.6 However, this would appear to put great faith in the various industry players being willing and equal in terms of bargaining power and leaves open the possibility that a data user will have to use multiple data sharing avenues (each with their own particular requirements) to deliver a holistic view of a customer's full financial position.

6.7 Risk of unauthorised access

6.8 Given the treasure trove of financial data that data users will have access to, data security, the risk of unauthorised access and fraud, and liability for such access, are key concerns for FiDA's implementation.

6.9 However, FiDA is less prescriptive than PSD2 in this regard. The Commission Text refers to "*appropriate levels of security*" for data transmission and storage, and the Parliament and Council Texts require FDSS to establish "*minimum technical and organisational measures members shall implement to ensure an appropriate level of security for exchanged data, including security measures to prevent and mitigate the risk of fraud*".

6.10 The risk is that FISPs and other data users not currently engaged in digital data sharing will present softer targets for bad actors and, in the case of FISPs, may not necessarily have the means to compensate customers in the event of a significant data breach (despite the requirements to have insurance to cover liability resulting from non-authorised or fraudulent access/use of data).

6.11 Requirements for strong security under DORA (the Digital Operational Resilience Act 2022/2554) mitigate some of the risk; however, the sheer wealth of data that can be mined as a result of FiDA presents a real shift in terms of the amount of damage that could result from a data breach in one place.

7. Monetising data (Article 10)

7.1 PSD2 explicitly prohibited inscope data holders (i.e. account servicing payment service providers) from charging TPPs. This "free access" mandate was intended to promote FinTech innovation; however, it proved to be a major point of contention with banks, who bore the cost of building and maintaining APIs without revenue from TPPs.

7.2 FiDA introduces a structured framework for monetisation that seeks to address this issue, but places limitations on data holders (e.g., banks, insurers, investment firms) can charge.

7.3 They can charge data users for access (but not the underlying consumers), provided such fees are part of an official FDSS. Where fees are specified in the FDSS, they must be reasonable, cost-based, and non-discriminatory.

7.4 Whilst this seems fair on the face of it, any cost for participation will have an impact on the balance sheets of those that participate. Those with the deepest pockets (e.g. FIs with income from existing financial service activities) will be better placed to absorb this cost. FISPs, on the other hand, might not have such flexibility.

7.5 It also means that data is worthy of valuable consideration under one data sharing regime (FiDA) but not the other (PSD2).

8. Dashboard (Article 8)

8.1 Data holders will be required to provide a "permissions dashboard" to enable customers to:

(a) monitor and manage the consents they provide to data users; and

(b) cancel and re-establish those consents in the data holder domain.

8.2 The three texts differ on the details of precisely what the dashboard must permit, but the overarching point is that data holders and users will be required to cooperate in real-time to ensure the information on the dashboard is live and to communicate changes in customer consent/new consents to each other.

8.3 Ideally, a single market solution would emerge, possibly as part of FDSS design(s), to deliver this functionality. However, this may well be difficult to achieve.

8.4 The use of a dashboard reflects a development seen in the PSR, and there appears to be movement towards aligning the two regimes:

(a) the Council text of the PSR proposed that TPP dashboards be consistent with FiDA equivalents, and to allow payment service users to manage data permissions pursuant to both the PSR and FiDA through a single dashboard.

(b) similarly, the Commission's Simplification Non-Paper suggested ensuring alignment of permission dashboards under FiDA and the PSR.

8.5 However, much remains to be resolved, and the risk is that one regulatory framework dictates the outcome for the other.

8.6 Data holders will be concerned about incurring significant cost, or having to carry out large-scale technology projects, to ensure compliance.

9. Penalties (Article 20)

9.1 The European Supervisory Authorities ("**ESAs**") are empowered to issue guidelines and oversee FDSS governance, with calls for strong penalties for breaches and strict controls on "dark-pattern consent techniques" (which the Digital Services Act (Regulation (EU) 2022/2065) describes as 'practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions').

9.2 Certain breaches are covered by both PSD2 and FiDA. However, FiDA introduces two new examples of breach:

	PSD2	FiDA
Unauthorised access to data/accounts	x	x
Failure to obtain valid consent	x	x
Technical non-compliance (e.g., bad APIs)	x	x
Misuse of data (e.g., using it for wrong purposes)	x	x
Dark patterns or manipulation of consent prohibited)		x
Charging consumers for access		x

9.3 However, both FiDA and the PSR are introducing a more uniform and draconian penalty regime for breach.

9.4 Article 103 of PSD2 provided that Member States should set and enforce penalties that are: *"effective, proportionate and dissuasive."* Whilst this didn't lead to light-touch penalties (e.g. in Germany, BaFin can impose multi-million euro fines), PSD2 did not set fixed amounts; thus penalties can vary widely by EU jurisdiction.

9.5 FiDA aligns its penalty structure much more closely with GDPR-style enforcement. Breaches of core obligations (e.g., consent misuse, illegal data access, failing to provide a permission dashboard), are punishable with fines and bans, including:

(a) maximum fines of at least two times the profits gained/losses avoided due to infringements (which can exceed fines for natural or legal persons below);

(b) €25,000 per infringement, up to a maximum of €250,000 per year for natural persons;

(c) a ban on individuals (potentially up to 10 years);

(d) €50,000 per infringement up to a max of €500,000 million or 2% of annual global turnover for firms, whichever is higher; and

(e) periodic penalties up to 3 % of average daily turnover, or €30,000 for natural persons, for ongoing breaches.

9.6 The Parliament and Council Texts increase these penalties, with the Council Text hitting highs of €5 million for both natural persons, and up to 10% of annual turnover for firms.

9.7 The increases reflect an approach proposed under the PSR, which introduces administrative fines of two times profits/losses avoided, or 10% on annual global turnover for firms and €5 million for natural persons, and the same concept and level of periodic penalties.

Authors

Eimear O Brien
Partner
eimear.obrien@hoganlovells.com

Charles Elliott
Counsel Knowledge Lawyer
charles.elliott@hoganlovells.com

Lavan Thasarathakumar
Senior Advisor
lavan.thasarathakumar@hoganlovells.com

Americas

- Boston
- Denver
- Greater Washington, D.C.
  - Baltimore
  - Washington, D.C. and Northern Virginia
- Houston
- Los Angeles
- Miami
- Minneapolis
- New York
- Philadelphia
- Northern California
  - San Francisco
  - Silicon Valley
- Latin America
  - Brazil
  - Mexico

Europe, Middle East and Africa

- Amsterdam
- Brussels
- Dublin
- Germany
  - Berlin
  - Düsseldorf
  - Frankfurt
  - Hamburg
  - Munich
- London
- Luxembourg
- Madrid
- Milan
- Rome
- Paris
- Middle East
  - Dubai
  - Riyadh

Asia Pacific

- Greater China
  - Beijing
  - Hong Kong
  - Shanghai
- South East Asia
  - Ho Chi Minh City
  - Jakarta
  - Singapore
- Tokyo

www.hoganlovells.com